The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
1/25/2011

SUBJECT:
Vulnerability in Novell GroupWise Internet Agent Could Lead to Remote Code Execution

OVERVIEW:
Novell GroupWise is a collaborative software product, which includes email, calendars, instant messaging and document management. A vulnerability has been discovered in Novell GroupWise Internet Agent. The GroupWise Internet Agent (GWIA) is a server component that provides communication to other email systems and conversion of email messages to GroupWise format. Successful exploitation could allow an attacker to gain SYSTEM-level privileges. An attacker could then install programs; view, change, or delete data; or create new accounts. Unsuccessful exploitation attempts may result in a denial of service.

SYSTEMS AFFECTED:
- Novell GroupWise Internet Agent
- Novell GroupWise 8.02 HP2 and earlier
- Novell GroupWise 7.04 and earlier
- Novell GroupWise 6.5 and earlier

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:
Novell has confirmed the existence of a buffer-overflow vulnerability in Novell GroupWise Internet Agent that may allow remote code execution with SYSTEM-level privileges. The GroupWise Internet Agent (GWIA) provides communication to other email systems and conversion of email messages to GroupWise format. The vulnerability occurs due to the way the Internet Agent processes 'VCALENDAR' data included in an email message, specifically the 'REQUEST STATUS' variable. The vulnerability exists within the 'gwwww1.dll' module responsible for parsing 'VCALENDAR' data within

messages. Exploitation occurs when a user views a carefully crafted malicious message. Successful exploitation of the vulnerability will lead to a completely compromised system. Unsuccessful exploitation attempts may result in a denial of service. Exploit code is not publically available at this time. Novell has supplied updates which fix this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Novell to vulnerable systems immediately after appropriate testing

REFERENCES:

Novell:

http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7007155&sliceId=1&docTypeID=DT_TID_1_1&dialogID=199990003&stateId=0%200%20199988016

Security Focus:

http://www.securityfocus.com/bid/45994

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4326

Zero Day Initiative:

http://www.zerodayinitiative.com/advisories/ZDI-11-025